criterion," and that this implies multiple sets of rules. No resolution was reached during the telephone conference.

In response, applicants again respectfully traverse the rejections to claims 1-26 for at least the reasons presented below. As contended in applicants' first Response dated November 12, 1999, in the telephone conference of March 27, 2000, and as reiterated below, applicants' respectfully assert that Shwed fails to teach or suggest the use of multiple security policies having respective rule sets as employed in accordance with the hierarchical approach of the claimed invention. Rather, Shwed employs a single rule set in the context of object groups.

The present invention is generally directed to methods and apparatus for providing a firewall service in a computer network wherein multiple domains and/or multiple security policies are supported. The security policies are represented by sets of access rules which may be loaded into the firewall by a system administrator. For example, in one embodiment, a single firewall supports multiple users, each with a separate security policy. The particular rule set that is then applied at the firewall for any packet may be determined based on some piece of information associated with the packet such as, for example, incoming and outgoing network interfaces, as well as network source and destination addresses. Thus, the invention effectively provides a hierarchical rule selection procedure. That is, before a rule is applied to a particular packet, the appropriate set of rules is first selected and then, a rule from the selected set is applied to the packet.

Shwed is a system for securing inbound and outbound data packet flow in a computer network by employing security rules in appropriately placed packet filters. Each packet filter may handle multiple security rules, as mentioned at column 4, lines 23-26. The Shwed system identifies hardware devices controlled by the packet filters as objects. These objects can be grouped depending on their application, e.g., finance department, research and development department, directors of a company protected by the system. Thus, Shwed permits the control of data flow not only to individual devices on its network, but also to groups of devices. One example of rule selection in accordance with such grouping ability is discussed at column 4, line 58-65. There it is explained that, in accordance with the Shwed system, it is possible to have the chief financial officer, as well as other higher ranking officials of the company, be able to communicate directly with the finance group, but filter out communications from other groups. Further, it is possible to allow e-mail from all groups, but to limit other requests for information to a specified set of computers. This is

accomplished by appropriate placement of packet filters and application of a single set of rules within each filter. That is, as explained at column 7, line 18+, a packet is received by a packet filter, compared with a security rule and a determination is made whether or not the packet matches the rule. If the packet matches the rule, a decision may be made to pass or drop the packet based on the requirements of the security rule. If the packet doesn't match the rule, then a next rule in the rule set is examined in a similar fashion. Thus, in a manner much like any conventional ordered rule set system, the Shwed system handles group requirements, such as those mentioned in the example above, by simply defining the rules in the single rule set in order to implement the group requirements.

Rule selection in the Shwed system is therefore significantly different than that provided by the claimed invention. As explained above, the invention provides for first selecting a rule set or security policy and then applying a rule from the set or policy.

Such a hierarchical approach is not obvious in view of Shwed for at least the following reasons. First, the methodology of the invention not only provides for greater rule selection and application flexibility, but also faster overall rule processing for a given packet. Further, independent rule administration is permitted by this methodology which is a major advantage over Shwed since Shwed would only permit one administrator to control all packet filter rules. Also, the present invention permits the downloading and thus updating of individual rule sets or policies without affecting other rule sets or policies in the same firewall.

Independent claim 1 recites the step of "selecting at least one of a plurality of security policies as a function of [a] session key" derived for a packet and then using the selected security policy in validating the packet. Independent claim 8 recites "designating a plurality of independent security policies, with each of the security policies including a set of access rules; determining which security policy is appropriate for the packet; and validating the packet using the set of access rules of the determined security policy." Independent claim 12 has similar limitations as claim 8. Independent claim 17 recites "means for selecting at least one of a plurality of security policies as a function of [a] data item" obtained from a request for a session and then using the selected security policy in validating packets of the session. Independent claim 22 has similar limitations as claim 17. Thus, each claim defines this novel rule selection approach based on first selecting a policy, e.g.,

set of rules, and then using the selected policy to process one or more packets. Shwed clearly fails to teach or suggest use of such multiple security policies.

Applicants' do not specifically see where Shwed refers to rules with "multiple criterion," as mentioned by the Examiner during the telephone conference of March 27, 2000. However, even assuming for argument sake that Shwed does disclose rules with "multiple criterion," this still does not teach or suggest the use of multiple security policies or rule sets according to the invention.

Lastly, independent claim 16 recites "segmenting access rules into a plurality of domains; and administering the access rules such that only an administrator for a given domain is permitted to modify rules of a security policy for that domain." Again, the claim defines multiple security policies through the segmentation of access rules into a plurality of domains. This is neither taught nor suggested in Shwed.

The Office Action contends that "[i]t would have been obvious to one of ordinary skill in the art, at the time the invention was made, to allow the creation of specific security rules for a particular sub-group of network objects, because this could be accomplished with little modification to the Shwed system, and because the creation of independent security policies by the creation of multiple sets of rules would give users of the Shwed system the benefits of hierarchies of security." However, applicants respectfully contend this is merely conclusory and, in any case, a hindsight application of the reference. As stated above, Shwed does no more than a conventional ordered rule set system in applying a single rule set to a packet wherein the rules of the set are simply defined to effectuate certain actions on a variety of objects. The fact that the objects may be partitioned into groups does not change the fact that only one rule set is used. There is no suggestion whatsoever to apply a hierarchical rule selection procedure as in the claimed invention.

Accordingly, it is respectfully asserted that independent claims 1, 8, 12, 16, 17 and 22 are patentably distinguishable over Shwed and therefore in condition for allowance. Also, due at least to their respective dependence on such independent claims, it is further respectfully asserted that claims 2-7, 9-11, 13-15, 18-21 and 23-26 are patentably distinguishable over Shwed and therefore

in condition for allowance. Reconsideration is respectfully requested. A Notice of Appeal is being filed concurrent with this Response.

Respectfully submitted,

William E. Lewis

Date: April 27, 2000

William E. Lewis
Attorney for Applicant(s)
Reg. No. 39,274
Ryan & Mason, L.L.P.
90 Forest Avenue
Locust Valley, NY 11560
(516) 759-2946